VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Absolvování individuální odborné praxe

Individual Professional Practice in the Company

13. srpna 2012

Ondřej Filip

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Ondřej Filip**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Tieto Czech s.r.o.
2. Struktura závěrečné zprávy:
   a) Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta.
   b) Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti.
   c) Zvolený postup řešení zadaných úkolů.
   d) Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe.
   e) Znalosti či dovednosti scházející studentovi v průběhu odborné praxe.
   f) Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení.

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vede odbornou praxi studenta.

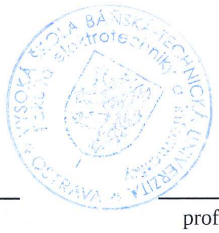
Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **doc. Dr. Ing. Eduard Sojka**

Konzultant bakalářské práce: mgr inż Michal Dressler

Datum zadání: 18.11.2011

Datum odevzdání: 04.05.2012



doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Obsah

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

13. 8. 2012 — V Ostravě dne

Ondřej Filip — Ondřej Filip

Abstrakt

Tato bakalářská práce popisuje individuální odbornou praxi v externím subjektu – společnosti Tieto Czech s.r.o. Podává základní informace o klíčových oblastech, ve kterých firma působí a popis mého pracovního zařazení. Pokračuje informacemi o pracovních úkolech prováděných během praxe a jejich řešení. V závěru reflektuje samotnou praxi ve vztahu ke znalostem a dovednostem získaným na univerzitě.

KLÍČOVÁ SLOVA: Tieto, Cisco, síťová zařízení

Abstract

This bachelor thesis describes individual professional practice in external company – Tieto Czech s.r.o. Basic information about key business areas where the company operates and description of my position in company is presented. Then information about tasks carried out during the practice follows. The thesis is concluded with part which reflects the practice itself in relation to knowledge and skills gained at the university.

KEYWORDS: Tieto, Cisco, network devices

Seznam použitých zkratek a termínů

ACL Access Control List – seznam pravidel, podle kterých se v zařízeních Cisco filtrují pakety

ASA Adaptive Security Appliance – síťové zařízení firmy Cisco, integruje funkce několika bezpečnostních zařízení

ASDM Adaptive Security Device Manager – aplikace pro správu zařízení Cisco ASA

CM Change Management – proces zodpovědný za kontrolu životního cyklu všech změn, primárním cílem tohoto procesu je umožnit provedení užitečných změn bez narušení IT služeb (Rance a Hanna, 2007)

CRM Customer Relations Management – proces při kterém se získávají a zpracovávají dat o firemních klientech, jejich obchodních vztazích se společností, slouží k pochopení požadavků a zvyků jednotlivých zákazníků, CRM systém je softwarovou implementací takového procesu

ECM Enterprise Content Management – soubor strategií, metod a nástrojů používaných pro zachycení, správu, uložení, zachování a doručení obsahu a dokumentů vztahujících se k organizačním procesům (AIIM, 2010)

ERP Enterprise Resource Planning – systém pro řízení informačních toků a procesů v rámci i vně společnosti

IDS Intrusion Detection System – program, který automatizuje proces monitorování událostí v počítačovém systému nebo síti a provádí analýzu získaných dat (Scarfone a Mell, 2007)

IPS Intrusion Prevention System – má všechny schopnosti systému IDS a navíc je schopen zabránit možným útokům (Scarfone a Mell, 2007)

ITIL Information Technology Infrastructure Library

ITSM Information Technology Service Management – implementace a správa kvality IT služeb, která odpovídá firemním požadavkům

NAT Network Address Translation – překlad cílových nebo zdrojových adres IP paketů

RDP Remote Desktop Protocol – protokol pro vzdálené připojení k sezení systémů Microsoft Windows

SLA Service Level Agreement – dohoda mezi poskytovatelem IT služeb a zákazníkem, popisuje službu a její úroveň, specifikuje odpovědnost smluvních stran (Rance a Hanna, 2007)

SSH Secure Shell – síťový protokol, také klient využívající tento protokol, slouží pro zabezpečený přenos dat, používá se pro připojení k shellu vzdálených zařízení nebo pro tunelování síťového provozu skrze šifrovaný kanál

VPN Virtual Private Network – virtuální privátní síť, prostředek pro spojení dvou uzlů přes veřejnou síť, který zprostředkovává přístup ke vzdáleným uzlům nebo lokálním počítačovým sítím a jejich službám, zpravidla jde o šifrované spojení

paketový filtr program, který filtruje síťový provoz podle nastavených pravidel, *stavový paketový filtr* je schopen ukládat informace o spojeních a otevřít kanál pro komunikaci patřící k povolenému provozu

routing též *routování, směrování*, činnost routeru (směrovače) – odeslání daného paketu na cílovou adresu nebo adresu dalšího routeru skrze odpovídající síťové rozhraní dle informací ve směrovací tabulce

shell interpret příkazů, program, který poskytuje textové rozhraní pro uživatele

ticket jde o instanci procesu, může nabývat různých jmen dle specifického procesu, pro Incident Management jde o „incident“, pro Change Management jde o „change“ (změnu)

0 Úvod

Obsahem této práce je popis průběhu praxe ve společnosti Tieto Czech s.r.o. Nejdříve je uvedeno několik základních informací o společnosti a jejím působení. Dále práce popisuje mé pracovní zařazení jako technického specialisty v kontextu celého podniku a jeho oddělení. V další části se zabývám pracovními úkoly, které jsem dostal v průběhu praxe a jak jsem přistoupil k jejich řešení. Práci uzavírá shrnutí znalostí získaných před nástupem do praxe stejně jako pojmenování znalostí chybějících, a též popis znalostí a vědomostí získaných během samotné praxe.

1 Odborné zaměření firmy

1.1 Tieto Corporation

Tieto je společnost působící na mezinárodní úrovni a poskytující služby v oblasti IT, poradenství a systémové integrace a také výzkumu a vývoje (R&D).

Společnost Tieto nabízí řešení, hotové platformy a konzultace v oblastech od správy infrasktruktury, přes správu aplikací, business plánování (ERP), řízení vztahu se zákazníky (CRM) až po řízení obsahu (ECM). Pro zákazníky, kterým nestačí existující softwarové balíky nabízí vyvinutí nových aplikací nebo přizpůsobení stávajících, tak aby odpovídaly kladeným požadavkům. Do této oblasti spadají také řešení pro testování software během celé doby jeho životního cyklu, včetně konzultací a ohodnocení stávajících zákaznických procesů pro vývoj software. Spolupracuje při tom s partnery jako je Microsoft, Oracle a SAP.

Jako doplněk dodávaných řešení Tieto zajišťuje outsourcing hardware i celých softwarových platforem. Zákazník může zvolit úroveň služby odpovídající jeho potřebám a tuto úroveň dále regulovat dle aktuálního vývoje. Součástí tohoto přístupu je nabídka optimalizace stávající IT infrastruktury.

Co se týká regionální působnosti, společnost se zaměřuje především na oblast severní a východní Evropy, ovšem má pobočky i v Indii, Číně a dalších zemích. Jednou z jejich filiálek je od roku 2001 Tieto Czech s.r.o.

1.2 Tieto Czech s.r.o.

Od roku 2004 působí Tieto Czech také v Ostravě. V současnosti se zde nachází pracoviště pro zhruba dva tisíce specialistů zabývajících se různými oblastmi IT.

2 Pracovní zařazení

Pro svou praxi jsem volil mezi oddělením serverových technologií na platformě Unix a oddělením síťových specialistů druhou možnost. Byl jsem přiřazen jako technický specialista k týmu síťových specialistů, zabývajícího se primárně prací pro švédské zákazníky. Celkem pracovalo v tomto týmu dvacet zaměstnanců. Vzhledem k celkově menšímu počtu zákazníků oproti finskému prostředí se tým zabýval širším spektrem činností.

Ve společnosti Tieto je na základě knihovny ITIL aplikován třívrstvý hierarchický model, ve kterém spadali mí kolegové do třetí nebo druhé vrstvy této architektury. Mé pracovní úkoly se pohybovaly především v rámci druhé vrstvy – řešení incidentů přijatých nižší vrstvou, úpravy v zákaznickém prostředí na žádost zákazníka, eskalace incidentů, které si žádají změnu architektury nebo vyžadují hlubší znalosti zákaznického prostředí, na třetí vrstvu. Třetí vrstva se zabývá pokročilou podporou a spoluprací se zákazníkem a řeší komplexní problémy v prostředí zákaznické nebo firemní infrastruktury.

Během své praxe jsem rovněž asistoval dalším kolegům v jejich práci na projektech týkajících se síťové infrastruktury.

3 Seznam úkolů a postup řešení

Většina úkolů v průběhu mé praxe spadala do oblasti síťových technologií. Výjimkou byly prvotní úkony vztahující se k pracovnímu prostředí a základním nástrojům používaným ve společnosti.

3.1 Základní seznámení s pracovními nástroji

3.1.1 Action Request System

Na úvod jsem se seznámil s desktopovou aplikací BMC Remedy User, což je rozhraní pro ITSM software BMC Remedy. Tato aplikace poskytuje data a rozhraní sloužící pro správu IT služeb. Aplikace umožňuje nejen správu incidentů a změn ve formě ticketů, ale také sledování „konfiguračních položek“, dále jen CI (configuration item). Za CI je považována každá komponenta, která musí být spravována, aby mohla být poskytnuta IT služba. Patří mezi ně další IT služby, hardware, software, budovy apod. Tato aplikace je používána v každodenním provozu a všichni pracovníci by ji měli ovládat.

Každý ticket je označen unikátním označením pro snadnou identifikace a má záznam vykonané činnosti (worklog) stejně jako řadu dalších informativních položek včetně vazeb na CI, zákazníka a SLA, do kterého ticket spadá. SLA definuje časový rámec ve kterém se na ticket musí zareagovat či dokdy je třeba ticket vyřešit. Informace poskytnuté v ticketu slouží pro snadnější nalezení příčin problémů, identifikaci CI a obsahují kontaktní údaje zákazníka.

Pro technického specialistu jsou nejpodstatnější incidenty, požadavky na změnu a tzv. akce ve formě ticketů. Tickety jsou přidělovány jednotlivým specialistům shift supervisorem, což je úloha, jejíž vykonávání buď rotuje mezi členy týmu anebo je náplní práce zvlášť určeného jednotlivce. Shift supervisor má k dispozici informace o tom, do jaké míry je daný pracovník seznámen s konkrétní lokalitou, případně jaké jsou jeho znalosti v dané problematice, a přiřazuje na základě těchto informací konkrétní tickety. Zároveň zohledňuje počet ticketů, které již má pracovník přiřazeny a jejich SLA.

3.1.2 Vzdálená připojení

Pro s právu vzdálených připojení na různá zařízení jsem využil aplikaci mRemote, která umožňuje přehledně organizovat vzdálená zařízení, na která se síťový specialista připojuje. Tyto zařízení mohou používat pro vzdálenou správu rozdílné technologie (SSH, telnet, RDP,...) a vyžadovat různé přihlašovací údaje a hesla. Pomocí mRemote je lze přehledně kategorizovat a zařadit. Používání tohoto programového prostředku je volitelné, ale je velmi doporučováno. Při objemu práce, který je v týmu denně zpracováván, se nevyplatí opakovaně dohledávat zařízení a ručně zadávat přihlašovací údaje.

3.1.3 Monitorování síťových zařízení

Jakákoli práce se zařízeními, o nichž nemá specialista dostatek informací, je velmi problematická. Proto je nutné, aby byla síťová zařízení a zařízení v síti monitorována. Sledované parametry a data mohou být uchovávány na konkrétních zařízeních nebo odesílána určenému serveru. Izolovaný sběr dat ovšem neumožňuje rychlý přehled o stavu sítě a také velmi zpomaluje proces vyhodnocování incidentů.

Proto je ve společnosti Tieto zaveden, jako jeden z několika monitorovacích systémů, software HP Network Node Manager i (dále NNMi). Během mé praxe jsem často využíval NNMi pro získání doplňujích informací. Tento software umožňuje agregovat data z velkého počtu sledovaných zařízení nebo-li uzlů a následně tyto data zpracovat pro další použití. Sběr dat ze samotných zařízení probíhá pomocí protokolu SNMP. Systém NNMi nabízí možnost přehledně zobrazit grafickou podobu síťové topologie spolu se stavem daných uzlů – lze tak rychle identifikovat možnou příčinu a místo incidentu. Vyhrazená část uživatelského rozhraní poskytuje informace o historickém vývoji sledovaných hodnot jako je například dostupnost zařízení nebo informace o poslední aktualizaci dat.

Pokud dojde k výpadku v určitém segmentu sítě, lze vysledovat průběh incidentu, případně události, které mu předcházely. Síťový specialista díky tomu může identifikovat neočekávané chování v daném síťovém segmentu a vymezit okruh dotčených zařízení a síťových segmentů, a to i zpětně.

3.2 Seznámení s architekturou síťové infrastruktury

V rámci tohoto úkolu jsem absolvoval školení o síťové infrastruktuře v rámci společnosti. Pan Dressler mi vysvětlil architekturu druhé a třetí síťové vrstvy. Prošel jsem s ním klíčové síťové prvky infrastruktury – páteřní switche, routery, VPN koncentrátory.

Získal jsem díky tomu představu o tom, jak funguje síťová infrastruktura – to je podstatné nejen pokud je potřeba provést úspěšné řešení incidentů, ale i při přidávání a odebírání různých částí infrastruktury – switche, servery apod.

3.2.1 Cisco Adaptive Security Appliance

Dalším krokem bylo školení pro práci se zařízeními Cisco ASA. Tyto síťové prvky jsou schopné zastupovat funkce stavového paketového filtru, mohou spravovat site-to-site nebo endpoint VPN spojení a mají i omezenou IPS funkcionalitu. Základem platformy ASA je upravený Linuxový kernel, na němž běží softwarová nádstavba, poskytující textové i grafické rozhraní. Textové rozhraní je velmi blízké operačnímu systému IOS, používaném v routerech a přepínačích firmy Cisco. Díky tomu je konfigurace při předchozí zkušenosti s se systémem IOS jednodušší. Textové rozhraní je silným nástrojem pro správu síťových zařízeních firmy Cisco, avšak při některých činnostech je vhodné použít grafické rozhraní. Platforma Cisco ASA pracuje s aplikací ASDM, jejíž pomocí lze provádět celkovou

správu zařízení. ASDM neběží přímo na zařízení, ale jde o tak zvaného „tlustého klienta“ napsaného v jazyce Java, který je spuštěn na počítači specialisty. Pomocí takového rozdělení jsou potlačeny možnosti útoku na zařízení skrze chyby v implementaci grafického rozhraní.

Během praxe jsem nejvíce pracoval právě se zařízeními na platformě Cisco ASA, zatímco s routery a přepínači na platformě IOS jen okrajově.

Po úvodních školeních jsem začal pracovat na ticketech přidělených shift supervisorem nebo konzultantem. Některé tickety jsem po dohodě převzal od kolegů v týmu.

3.2.2 Virtualizace síťových prvků

Za účelem zafixování znalostí a otestování chování zařízení při různých konfiguracích jsem pomocí open-source simulátoru sítí GNS3 nasimuloval modelovou síť se zařízeními Cisco ASA v redundantním zapojení spolu se standardními routery se systémem Cisco IOS. Simulaci jsem využíval opakovaně k ověření teoretických postupů a k dalšímu vzdělávání.

Aplikace GNS3 je grafickou nádstavbou pro aplikace Dynamips a Qemu – tyto se starají o vlastní simulaci hardwaru nutného pro běh simulovaných zařízení. GNS3 dovoluje simulovat omezenou množinu síťových zařízení od různých výrobců a ukládání jejich konfigurací i ucelených virtuálních topologií. Při své praxi jsem využil také schopnost integrace virtuálních počítačů vytvořených virtualizačním softwarovým balíkem VirtualBox. Lze takto připravit servery, které nabízejí služby pro klientské virtuální počítače a simulují reálný provoz, procházející sítí.

Zatímco pro routery a Cisco ASA platformu nabízí GNS3 virtuální hardware, na kterém může běžet software pro daná zařízení, podpora virtualizace pro přepínače chybí protože specifikace speciálních obvodů, použitých pro realizaci funkcí přepínače, nejsou veřejně dostupné.

3.3 Řešení zákaznických požadavků a incidentů

Zákaznické požadavky jsou nejčastěji specifikované ve formě tzv. CM ticketů, které se skládají z několika AC ticketů – po úspěšném dokončení všech akcí je dosaženo požadované změny – např. přidání serveru do zákazníkovy sítě.

Prvním krokem při řešení ticketu je identifikace zákazníka a nalezení odpovídající dokumentace v informačních systémech pro sdílení dat. Poté následuje identifikace síťového provozu, který dané zařízení bude vyžadovat. Se znalostí provozu lze snáze zkontrolovat routing mezi sítí zákazníka a dalšími prostředími, kterými a do nichž síťové spojení zasahuje. Pokud např. směrovací tabulky obsahují danou síť s jinou masku než má cílová síť, spojení nemusí být úspěšné, protože se routery budou rozhodovat podle nekonzistentních informací a nedoručí pakety na místo určení.

Stejný princip platí u povolení síťového provozu, kdy je třeba zkontrolovat povolení provozu stejně jako překlad (NAT) adres na korektní adresu, která je na straně zákaznického firewallu očekávaná.

Mohou nastat v zásadě dvě situace – síťové prvky již jsou nakonfigurovány protože server patří do existující serverové farmy, která má povoleny odpovídající spojení, nebo je server prvním v dané lokalitě a je nutné pro něj nová pravidla vytvořit. Druhý případ vyžaduje větší míru pozornosti a porozumění fungování síťe u daného zákazníka. V případech, kdy jsem nebyl schopen ani s pomocí dokumentace vyřešit daný požadavek, obrátil jsem se na ostatní kolegy, kteří byli za danou lokalitu zodpovědní. Ti mé případné dotazy zodpověděli a pomohli mi s orientací v prostředí daného zákazníka.

Řešení incidentů může být velmi podobné řešení AC ticketů, pokud je předmětem nefunkční spojení. Během kontroly routingu a pravidel na firewallu hledá technik přesnou příčinu incidentu a případně změní konkrétní pravidla nebo doplní směrovací tabulky. Ovšem v některých případech je identifikování příčiny značně ztíženo, protože se vyskytuje jen u určitého software, běžícího na serverech nebo koncových stanicích zákazníka. V takových případech je dalším východiskem kontaktování zákazníka a dotázání se na další podrobnosti, které mohou pomoci určit příčinu incidentu a případně stanovit opatření pro zamezení jeho opakování – ať už je to upravení parametrů aplikace nebo síťového zařízení.

3.3.1 Příklad řešení požadavku

Jako ilustrační případ jsem zvolil problém u zákazníka – obecního úřadu jistého města.

Na začátku zákazník vznesl požadavek na vytvoření nového virtuálního serveru pro své potřeby. V procesu CM mi bylo přiřazeno několik ticketů pro různé akce: rezervaci ip adresy, povolení komunikace mezi zákaznickou sítí a sítí Tieta a přiřazení portu do správné VLAN.

Po rezervování statické IP adresy a zařazení portu, na kterém byl připojen virtuální server jsem pokračoval v nastavení zařízení. Pro zákazníka nebylo použito zařízení ASA, místo toho zde byl jeden hraniční router Cisco s aktivními filtrovacími funkcemi. Zde byla v rozporu konfigurace ethernetového rozhraní routeru a přístupových seznamů (dále ACL). ACL a rozhraní sice pracovaly se stejnou IP adresou zákaznické sítě, avšak na rozhraní byla nastavena maska sítě s délkou 28 bitů oproti 29 bitům v ACL. Upravil jsem tedy po diskuzi s kolegou všechny ACL, kde se předpokládalo zahrnutí celé sítě tak, aby používaly masku s délkou 28 bitů. Z hlediska hraničního routeru a připojeného serveru se konfigurace jevila kompletní.

Ovšem během následného rozhovoru s kolegou, který je zodpovědný za instalaci a funkčnost serveru, bylo zřejmé, že se server nespojí se servery z infrastrukury Tieta, které zajišťují specifické služby. Ukázalo se, že napříc vnitřní síti Tieta neměly odpovídající routery a Cisco ASA zařízení ve směrovací tabulce záznam pro zákaznickou síť se správnou maskou. Po úpravě dotčených směrovacích tabulek se provoz již rozběhl.

Další testování ukázalo, že se s nově instalovaným serverem nemohou spojit servery na straně zákazníka, ležící za zákazníkovým firewallem mimo působnost Tieta. Vzhledem k tomu, že na straně Tieta byla zařízení nastavena odpovídajícím způsobem, uzavřel jsem své tickety pro akce jako Completed (hotové) s poznámkou, aby pro další problémy vytvořil zákazník nový ticket.

Ve výsledku jsme po domluvě se specialistkou ze Švédska doporučili zákazníkovi zkontrolovat nastavení překladu adres na jejich firewallu. Ukázalo se, že zde nastavený NAT pracuje také pouze s podmnožinou sítě. Zaměstnanci zákazníka odpovědní za toto zařízení následně provedli opravu, která umožnila odpovídající komunikaci projít firewallem. Celá příčina problému pravděpodobně souvisela s tím, že v počátku byla nakonfigurována na zákazníkově firewallu a v routerech jen podsíť celého rozsahu adres. Díky tomu, že zákazník měl při prvotní konfiguraci pouze malý počet serverů, které využily adresy jen z této podsítě, nebyl problém zřetelný až do okamžiku alokace adresy pro nový server.

3.4 Práce na projektech

Během své praxe jsem pracoval spolu s dalšími kolegy na několika projektech v rámci společnosti.

3.4.1 Mapování využití přepínačů

V rozsáhlých sítích může v průběhu času a po určitém množství změn dojít k nekonzistenci mezi dokumentací či databází a skutečným stavem. Pracoval jsem na projektu, jehož cílem bylo zmapovat rozdělení portů na přepínačích pro jednotlivé zákazníky a jejich servery oproti zdokumentovanému stavu.

Dosavadní postup v tomto případě znamenal připojit se k n přepínáčům a n-krát zadat přihlašovací údaje a příkaz ke vstupu do privilegovaného režimu následovaný příkazem k výpisu stavu portů na daném zařízení. Následně bylo nutné zkopírovat tento výpis a uložit do dokumentace pouze relevantní informace. Takový postup byl značně neefektivní a náchylný ke vzniku chyb. Rozhodl jsem se proto použít nástroj, který umožní zaznamenat textový proud při připojení pomocí protokolu Telnet nebo SSH, a zároveň bude příkazy provádět pro větší množinu zařízení najednou. Ze své zkušenosti jsem znal aplikaci ClusterSSH, která umožňuje replikaci příkazů pro více SSH spojení. Aplikace ClusterSSH je ovšem dostupná pouze pro operační systém GNU/Linux. Po určité době hledání se mi podařilo najít uspokojivé řešení pro platformu Microsoft Windows za pomoci aplikace PuTTYCS.

Díky tomuto řešení jsem mohl v jednom kroku získat informace až ze šestnácti zařízení. Tento limit byl dán množstvím oken programu PuTTY, které bylo možné zobrazit na monitoru beze ztráty možnosti kontroly úspěšného získání dat. Výstup jsem nastavil v klientovi PuTTY tak, aby pro každou IP adresu vytvořil soubor s textovým proudem celé relace.

Po získání výstupů ze všech přepínačů jsem použil nástroj grep pro vyhledání relevantních částí výstupu pomocí regulárních výrazů. Výsledkem byl daný počet souborů s názvy odpovídajícími IP adrese přepínače a obsahující popis konfigurace portů vhodný pro vložení do dokumentace.

3.4.2 Získání dat o úspěšnosti řešení požadavků

Pokud zákazník potřebuje upravit konfiguraci firewallu, který je spravován společností Tieto, zadá požadavek na povolení komunikace mezi určitými uzly na síti (servery, uživatelská PC apod.) do interního systému. Pro účely tohoto textu budu uvádět tento systém jménem FWSYS. V okamžiku, kdy klient do systému vloží svůj požadavek, je také vytvořen ticket v ARS systému, který obsahuje odkaz na webové rozhraní FWSYS. Pro jeden ticket v ARS systému může existovat více požadavků.

Samotný požadavek se může v systému FWSYS nacházet v několika stavech. Jedním z nich je stav „REJECTED“ (odmítnut). Do tohoto stavu se požadavek dostane, pokud jeho řešení nebylo schváleno zákazníkem nebo zodpovědnou osobou. Pro nás je postačující, pokud víme, že jednou z příčin zařazení požadavku do této kategorie může být nekorektní řešení požadavku.

V ARS sytému se ovšem stav požadavků neodrazí, takže není možné na základě vyhledávání zjistit počet ticketů, jejichž odpovídající požadavek ve FWSYS systému je ve stavu „REJECTED“ či jiném. Znalost počtu požadavků v daném stavu oproti jejich celkovému množství byla důležitá pro projekt kolegy, který se snažil posoudit efektivitu při řešení zákaznických požadavků.

Oba dva systémy – ARS BMC Remedy i FWSYS, jsou architektonicky odlišné aplikace. První z nich je velká aplikace externího dodavatele s množstvím funkcí pro různé případy užití, zatímco FWSYS, vyvinutý interně, je orientovan na specifické úkoly a jeho architektura je optimalizovaná tímto směrem. Vzhledem k omezeným možnostem změn v kódu FWSYS a nutnému schvalovacímu procesu, tak aby bylo možné data z obou systému propojit, bylo třeba zvolit řešení ležící mimo tyto systémy. Dalším omezením, daným bezpečnostními požadavky, byla nemožnost vznášet SQL dotazy přímo na databázi FWSYS. Protože FWSYS je aplikace s webovým rozhraním, bylo nutné simulovat chování uživatele, který zjistí, zda existuje pro daný ticket záznam ve FWSYS a následně zjistí také stav takového záznamu.

Exportování dat z ARS systému bylo poměrně snadné, protože systém poskytuje možnost vyhledávání pomocí vyhledávacího řetězce využívající pseudo SQL kód. Napsal jsem tedy vyhledávací řetězec pro vypsání všech relevantních ticketů za daný měsíc – výsledná tabulka byla pro můj skript exportována do CSV formátu.

Výstup dat z FWSYS byl komplikovanější. Pro práci ve FWSYS je totiž nutné provést autentizaci skrze HTML formulář. Samotnou činnost prováděla aplikace cURL, jejíž instance spouštěl skript pro shell BASH. Po počátečních problémech, způsobených neznalostí korektních hodnot některých proměnných odesílaných ve formuláři, se mi podařilo sestavit

správnou sekvenci dotazů a nastavit úložiště pro HTTP cookies soubory. Díky tomu mohla aplikace cURL přistupovat na stránky vyžadující autentizaci a udržet si SSL sezení po celou dobu komunikace s FWSYS.

Skript si nejdříve vyžádal přihlašovací údaje klienta (existujícího uživatele FWSYS) – v okamžiku, kdy aplikace cURL již měla ustavené SSL sezení a pro FWSYS se jevila jako přihlášený klient, začal skript v cyklu posílat vyhledávací formulář a přijímat výpisy požadavků, vrácených serverem. Ve skriptu byl nastaven interval po kterém došlo k pozastavení na náhodný časový interval, aby nedošlo k zahlcení serveru. Pokud byl nalezen nenulový počet záznamů, skript pomocí dalšího volání cURL zjistil stav jednotlivých požadavků a na konci provedl výpis informací o odpovídajících ticketech a požadavcích spolu s jejich počtem.

Díky získaným informacím byl schopen můj kolega vyčíslit počet požadavků, které bylo nutné znovu zpracovat a analyzovat vývoj této hodnoty v čase.

4 Znalosti a dovednosti

4.1 Uplatněné během praxe

Základní znalost síťových technologií jsem si upevnil v předmětu „Počítačové sítě“, kde se ukázaly kurzy CCNA a CCNP, pořádané na půdě univerzity, jako velmi dobrou investicí do vlastních znalostí.

Prvkem nutným pro mou praxi byla znalost teorie směrování a přepínání stejně jako detailní porozumění fungování TCP spojení nebo filtrování IP paketů.

4.2 Postrádané během praxe

Během praxe jsem si doplnil své vědomosti z oblasti síťových technologií o podrobnou znalost platformy Cisco ASA a získal praktické zkušenosti s její konfigurací. Díky kontaktu se zákazníkem a řešení jeho problémů jsem získal zkušenosti a poznatky ohledně identifikace a analýzy problémů, které mohou vznikat v síťové infrastruktuře.

Dále jsem začal využívat efektivních nástrojů pro zjednodušení často opakovaných úkonů a úkonů prováděných na velkém množině vzdálených zařízení. Naučil jsem se také chápat úlohu, kterou hraje aktuální a podrobná dokumentace při spolupráci ve firemním prostředí. Obecně jsem díky této praxi mohl uplatnit teoretické znalosti z oblasti síťových technologií.

Získal jsem dobrou představu a konkrétní zkušenosti s prací v nadnárodní společnosti, kde nedílnou součástí této práce tvoří komunikace v angličtině se zákazníkem nebo kolegy ze zahraničí. Toto lze na půdě školy suplovat jen těžko – z této stránky mohu kladně hodnotit svůj roční pobyt na stáži ve finské Lappeenrantě. Praxe ve společnosti Tieto znamenala uvedení poměrně teoretických znalostí do kontextu reálného nasazení.

Literatura

1 Rance, S. a Hanna, A. *Glossary of Terms and Definitions, ITIL© V3 Glossary*. v01 ed. [APM Group Ltd.], 2007. Dostupné z: http://www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx

2 AIIM *What is Enterprise Content Management (ECM)?*. AIIM [Association for Information and Image Management], 2010. Dostupné z: http://www.aiim.org/What-is-ECM-Enterprise-Content-Management.aspx

3 Scarfone, K. a Mell, P. *Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST Special Publication 800-94)*. NIST [National Institute of Standards and Technology], 2007. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf